John Heenan
Joseph P. Cook
HEENAN & COOK
1631 Zimmerman Trail
Billings, MT 59102
Phone: (406) 839-9091
Fax: (406) 839-9092
john@lawmontana.com
joe@lawmontana.com

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
GREAT FALLS DIVISION

ALLISON SMELTZ et al., on behalf of herself and all others similarly situated, Plaintiff, vs. LOGAN HEALTH and DOES I through X, Defendants.	Cause No. CV-22-28-GF-BMM-JTJ Judge **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Allison Smeltz (Plaintiff), individually and on behalf of the proposed class described herein, brings this action against Defendant Logan Health, and submits their Complaint and Demand for Jury Trial as follows:

INTRODUCTION

1. Plaintiff brings this action against Logan Health for its failure to protect her sensitive personal information, and the sensitive personal information of others similarly situated. Logan Health had access to such information through contracts it had with health care providers.

PARTIES

2. Plaintiff is a resident of Montana.

3. Logan Health is a domestic non-profit corporation.

4. Doe Defendants I through X are subsidiary, sister, or related entities of Logan Health who may be determined through discovery to bear responsibility for the actions described herein.

JURISDICTION & VENUE

5. The Court has diversity jurisdiction as the parties are residents of different states and the amount in controversy exceeds $75,000.

COMMON ALLEGATIONS

6. In February of 2022, Logan Health reported a data breach that compromised the personal identifying information ("PII") and protected health information ("PHI") of approximately 213,545 people including 174,761 Montanans. According to the notice, different information may have been compromised including name, address, medical record number, date of birth,

telephone number, email address, diagnosis and treatment codes, dates of service, treating/referring physician, medical bill account number and/or health insurance information, and Social Security numbers.

7. According to the notice, the breach occurred on November 18, 2021 and on November 22, 2021, Logan Health discovered suspicious activity including evidence of unauthorized access to a file server containing patient information. According to a Logan Health spokesperson, the perpetrator of the hack was a "malicious actor."

8. This data breach isn't the first time Logan Health has allowed patient information to be compromised. The hospital has also previously reported a January 2021 data breach to the Montana Attorney General's Office that affected 2,081 Montanans. In 2019, Logan Health, under its previous name of Kalispell Regional Healthcare, reported a breach to the Montana AG's Office that affected 126,805 Montanans. Following the 2019 breach, Logan Health claimed to be taking "further steps to revise procedures that will minimize the risk of a similar event happening again" and that "We...have taken steps to prevent similar events from occurring in the future."

9. The 2021 data breach occurred because, despite representations to the contrary, Logan Health failed to implement adequate and reasonable training of

employees and/or procedures and protocols which would have prevented the data breach from occurring.

10. Logan Health has identified Plaintiff as a victim of the data breach and has sent Plaintiff a letter informing her of such.

11. Logan Health was aware, or reasonably should have been aware, that a patient's sensitive personal information is of significant value to those who would use it for wrongful purposes.

12. A "cyber black market" exists in which criminals openly post stolen social security numbers and other personal information on multiple underground websites. Identity thieves can use sensitive personal information, such as that of Plaintiff and others similarly situated, to perpetrate a variety of crimes. According to the FBI Cyber Division, in an April 8, 2014 Private Industry Notification:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.

13. Logan Health was aware, or reasonably should have been aware, that health care organizations such as it are a prime target of "malicious actors" hoping to gain access to PII and PHI.

14. The ramifications of Logan Health's failure to keep the affected patients' sensitive personal information secure are long lasting and severe. Once

sensitive personal information is stolen, fraudulent use of that information and damage to the affected patients may continue for years. As explained by the Federal Trade Commission:

> Medical ID thieves may use your identity to get treatment – even surgery – or to bilk insurers by making false claims. Repairing damage to your good name and credit record can be difficult enough, but medical ID theft can have other serious consequences. If a scammer gets treatment in your name, that person's health problems could become a part of your medical record. It could affect your ability to get medical care and insurance benefits and could even affect decisions made by doctors treating you later on. The scammer's unpaid medical debts also could end up on your credit report.[1]

Also, as reported by CreditCards.com:

> The Ponemon Institute found that 36 percent of medical ID theft victims pay to resolve the issue, and their out-of-pocket costs average nearly $19,000. Even if you don't end up paying out of pocket, such usage can wreak havoc on both medical and credit records, and clearing that up is a time-consuming headache. That's because medical records are scattered. Unlike personal financial information, which is consolidated and protected by credit bureaus, bits of your medical records end up in every doctor's office and hospital you check into, every pharmacy that fills a prescription and every facility that processes payments for those transactions.[2]

The average time spent by those respondents who successfully resolved their situation was more than 200 hours, working with their insurer or healthcare

---

[1] Federal Trade Commission, *Medical ID Theft: Health Information for Older People*, available at www.consumer.ftc.gov/articles/0326-medical-id-theft-health-information-older-people (accessed November 8, 2019).

[2] Cathleen McCarthy, CreditCards.com, *How to Spot and Prevent Medical Identity Theft*, available at www.creditcards.com/credit-card-news/spot-prevent-medical-identity-theft-1282.php (accessed November 8, 2019).

provider to make sure their personal medical credentials were secure and verifying the accuracy of their personal health information, medical invoices and claims, and electronic health records. Indeed, fifty-nine percent (59%) of the respondents reported that their information was used to obtain healthcare services or treatments, and fifty-six percent (56%) reported that their information was used to obtain prescription pharmaceuticals or medical equipment. Forty-five percent (45%) of respondents said that the medical identity theft incident had a negative impact on their reputation, primarily because of embarrassment due to the disclosure of sensitive personal health conditions (89% of the respondents), thirty-five percent (35%) said the person committing the fraud depleted their insurance benefits resulting in denial of valid insurance claims, and thirty-one percent (31%) said they lost their health insurance entirely as a result of the medical identity theft. Twenty-nine percent (29%) of the respondents reported that they had to make out-of-pocket payments to their health plan or insurer to restore coverage. Additionally, the study found that almost one-half of medical identity theft victims lose their healthcare coverage as a result of the identity theft, almost one-third have their insurance premiums rise, and forty percent (40%) were never able to resolve their identity theft.

15. According to Logan Health's letter, it is offering affected patients 12 months of identity theft protection services. Such an offer is inadequate to protect

Plaintiff and others similarly situated. A free credit report and the ability to freeze their accounts is not only a right that every citizen enjoys, it is grossly inadequate to protect the Plaintiff and Class members from the threats they face resulting from the PII/PHI that was exposed. Moreover, although credit monitoring can help detect fraud after it has already occurred, it has very little value as a preventive measure and does nothing to prevent fraudulent tax filings. As noted by security expert Brian Krebs, "although [credit monitoring] services may alert you when someone opens or attempts to open a new line of credit in your name, most will do little — if anything — to block that activity. My take: If you're being offered free monitoring, it probably can't hurt to sign up, but you shouldn't expect the service to stop identity thieves from ruining your credit."

1. As a result of Logan Health's failures to prevent the Data Breach, Plaintiff and Class members have suffered and will continue to suffer damages. They have suffered or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII/PHI;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent,

detect, contest and recover from identity theft and fraud;

d. The continued risk to their PII/PHI, which remains in the possession of Logan Health and is subject to further breaches so long as Logan Health fails to undertake appropriate measures to protect the PII/PHI in their possession; and

e. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members.

16. Logan Health continues to hold the PII/PHI of its patients, including Plaintiff and Class members. Particularly because Logan Health has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class members have an undeniable interest in ensuring that their PII/PHI is secure, remains secure, and is not subject to further theft.

CLASS ACTION ALLEGATIONS

17. Plaintiff brings this lawsuit as a class action on her own behalf and on behalf of all other persons similarly situated as members of the proposed Class, pursuant to Federal Rules of Civil Procedure 23(a) and (b)(3), and/or (b)(1), (b)(2), and/or (c)(4). This action satisfies the numerosity, commonality, typicality, predominance, and superiority requirements.

18. The proposed Class is defined as:

> All persons whose sensitive personal information was compromised as a result of the breach of Logan Health's electronic information systems excluding any Judge or court staff presiding over the case.

Plaintiff reserves the right to modify, change, or expand the Class definition, including proposing additional subclasses, based on discovery and further investigation.

NUMEROSITY AND ASCERTAINABILITY

19. The size of the Class cannot yet be estimated with reasonable precision, but the number is great enough that joinder is impracticable.

20. The disposition of the Class members' claims in a single action will provide substantial benefits to all parties and to the Court.

21. The Class members are readily ascertainable from information and records in the possession, custody, or control of Logan Health. Notice of this action can be readily provided to the Class.

TYPICALITY

22. Plaintiff's claims are typical of the claims of all Class members in that the sensitive personal information of the representative Plaintiff, like that of all Class members, was compromised in the Data Breach.

ADEQUACY OF REPRESENTATION

23. Plaintiff is a member of the proposed Class and will fairly and

adequately represent and protect its interests. Plaintiff's counsel are competent and experienced in class action and privacy litigation and will pursue this action vigorously. Plaintiff has no interests contrary to or in conflict with the interests of the other Class members.

PREDOMINANCE OF COMMON ISSUES

24. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual Class members. Among the questions of law and fact common to the Class are:

a. Whether Logan Health had a duty to implement reasonable cyber security measures to protect Plaintiff and Class members' sensitive, personal information and to promptly alert them if such information was compromised;

b. Whether Logan Health breached its duties by failing to take reasonable precautions to protect Plaintiff and Class members' sensitive personal information;

c. Whether Logan Health acted negligently by failing to implement reasonable data security practices and procedures;

d. Whether Logan Health's failures to implement reasonable data security practices and procedures and to timely notify Plaintiff and Class members of the Data Breach violates Montana's Consumer Protection Act.

SUPERIORITY

25. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Absent a class action, most Class members would likely find the cost of litigating their claims prohibitively high and would have no effective remedy. Because of the relatively small size of the individual Class members' claims, it is likely that few, if any, Class members could afford to seek redress for Defendants' violations.

26. Class treatment of common questions of law and fact would also be a superior method to piecemeal litigation in that class treatment will conserve the resources of the courts and will promote consistency and efficiency of adjudication.

27. Classwide declaratory, equitable, and injunctive relief is appropriate under Rule 23(b)(1) and/or (b)(2) because Logan Health has acted on grounds that apply generally to the Class, and inconsistent adjudications would establish incompatible standards and substantially impair the ability of Class members and Defendants to protect their respective interests. Classwide relief assures fair, consistent, and equitable treatment of Class members and Defendants.

FIRST CAUSE OF ACTION
Negligence

28. Plaintiff incorporates the above allegations as if fully set forth herein.

29. Logan Health collected of Plaintiff and the Class members their names, physical addresses, dates of birth, health conditions, diagnoses, claims information, dates of service, and PII and PHI identifications (which may have included their social security numbers). Logan Health therefore owed Plaintiff and Class members a duty of reasonable care to preserve and protect the confidentiality of the sensitive personal information they collected. This duty included, among other obligations, taking reasonable security measures to safeguard and adequately secure from unauthorized access the sensitive personal information of Plaintiff and the Class members.

30. Plaintiff and the Class members were the foreseeable victims of Logan Health's inadequate cyber security. The natural and probable consequence of Logan Health failing to adequately secure its information networks was the unauthorized access of Plaintiff's and the Class members' sensitive personal information.

31. Logan Health knew or should have known that Plaintiff's and the Class members' sensitive personal information was an attractive target for cyber thieves.

32. Logan Health has the ability to sufficiently guard against data breaches.

33. Logan Health breached its duty to exercise reasonable care in protecting Plaintiff's and the Class members' sensitive personal information by failing to take reasonable security measures to safeguard and adequately secure from unauthorized access the sensitive personal information of Plaintiff and the Class members.

34. There is a close connection between Logan Health's failure to employ reasonable security protections and the injuries suffered by Plaintiff and the Class members. When an individual's sensitive personal information is stolen, she faces a heightened risk of identity theft and need to: (1) purchase identity protection, monitoring, and recovery services; (2) flag asset, credit, and tax accounts for fraud, including by reporting the theft of her social security numbers to financial institutions, credit agencies, and the IRS; (3) purchase or otherwise obtain credit reports; (4) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries and charges; (5) place and renew credit fraud alerts on a quarterly basis; (6) contest fraudulent charges and other forms of identity theft; (7) repair damage to credit and financial accounts; and (8) take other steps to protect themselves and recover from identity theft and fraud.

35. As a result of Logan Health's negligence, Plaintiff and the Class members have suffered damages that have included or may, in the future, include,

without limitation: (1) loss of the opportunity to control how their sensitive personal information is used; (2) diminution in the value and use of their sensitive personal information entrusted to Logan Health with the understanding that Logan Health would safeguard it against theft and not allow it to be accessed and misused by third parties; (3) the compromise and theft of their sensitive personal information; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and unauthorized use of financial accounts; (5) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including increased costs to use credit, credit scores, credit reports, and assets; (6) unauthorized use of compromised sensitive personal information to open new financial and other accounts; (7) continued risk to their sensitive personal information, which remains in Logan Health's possession and is subject to further breaches so long as Logan Health fails to undertake appropriate and adequate measures to protect the sensitive personal information in its possession; and (8) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach.

SECOND CAUSE OF ACTION
Invasion of Privacy (Intrusion Upon Seclusion)

36. Plaintiff incorporates the above allegations as if fully set forth herein.

37. Plaintiff and the Class members reasonably expected that the sensitive

personal information entrusted to Logan Health would be kept private and secure and would not be disclosed to any unauthorized third party or for any improper purpose.

38. Logan Health unlawfully invaded the privacy rights of Plaintiff and the Class members by:

a. failing to adequately secure their sensitive personal information from disclosure to unauthorized third parties or for improper purposes;

b. enabling the disclosure of personal and sensitive facts about them in a manner highly offensive to a reasonable person; and

c. enabling the disclosure of personal and sensitive facts about them without their informed, voluntary, affirmative, and clear consent.

39. A reasonable person would find it highly offensive that Logan Health, having collected Plaintiff's and the Class members' sensitive personal information, failed to protect that information from unauthorized disclosure to third parties.

40. In failing to adequately protect Plaintiff's and the Class members' sensitive personal information, Logan Health acted in reckless disregard of their privacy rights. Logan Health knew or should have known that its ineffective security measures, and the foreseeable consequences thereof, are highly offensive to a reasonable person in Plaintiff's and the Class members' position.

41. Logan Health violated Plaintiff's and the Class members' right to

privacy under the common law.

42. Logan Health's unlawful invasions of privacy damaged Plaintiff and the Class members. As a direct and proximate result of Logan Health's unlawful invasions of privacy, Plaintiff and the Class members suffered significant anxiety and distress, and their reasonable expectations of privacy were frustrated and defeated.

THIRD CAUSE OF ACTION
Breach of Implied Contract

43. Plaintiff incorporates the above allegations as if fully set forth herein.

44. As a condition of their use of Logan Health's services, Plaintiff and Class members were required to provide their PII and PHI including names, addresses, dates of birth, social security numbers and various health related information to Logan Health.

45. Plaintiff and Class members paid money to Logan Health in exchange for services, as well as Logan Health's promises to protect their protected PII and PHI from unauthorized disclosure.

46. Logan Health promised in its written prvacy policies that it would only disclose protected health information and PII under certain circumstances, none of which relate to the Data Breach.

47. Logan Health promised to comply with HIPAA standards and to make sure that Plaintiff and Class members' protected health information and PII would

be protected.

48. Implicit in the agreements between Logan Health and Plaintiff and Class members was Logan Health's obligation to: (1) use the PII of its patients for legitimate business purposes only, (2) take reasonable steps to secure and safeguard the protected health information and other PII, (3) not make unauthorized disclosure of such information, and (4) provide prompt and sufficient notice of any and all unauthorized access and/or theft of their protected health information and PII.

49. Logan Health breached the implied contract with Plaintiff and Class members by: (1) failing to reasonably safeguard and protect PII, (2) failing to comply with HIPAA, (3) failing to ensure confidentiality and integrity of PII and PHI, and/or (4) failing to protect against any reasonably anticipated threats of hazards to the security or integrity of protected health information.

50. Plaintiff and Class members have been damaged as a result of Logan Health's breach.

FOURTH CAUSE OF ACTION
Montana Consumer Protection Act

51. Plaintiff incorporate the above allegations as if fully set forth herein.

52. Logan Health is a person within the meaning of the Montana Consumer Protection Act and it conducts "trade" and "commerce" within the meaning of the Act.

53. Plaintiff and the Class members are "persons" within the meaning of the Act.

54. Logan Health engaged in unfair or deceptive acts or practices in the conduct of its business by the conduct set forth above. These unfair or deceptive acts or practices include the following:

a. failing to adequately secure Plaintiff's and the Class members' sensitive personal information from disclosure to unauthorized third parties or for improper purposes;

b. enabling the disclosure of personal and sensitive facts about Plaintiff and the Class members in a manner highly offensive to a reasonable person;

c. enabling the disclosure of personal and sensitive facts about Plaintiff and the Class members without their informed, voluntary, affirmative, and clear consent;

d. omitting, suppressing, and concealing the material fact that Defendant did not reasonably or adequately secure Plaintiff's and the Class members' sensitive personal information; and

e. Failing to disclose the Data Breach in a timely and accurate manner.

55. As a direct and proximate result of Logan Health's unfair or deceptive

acts or practices, Plaintiff and the Class members have suffered injury in fact and lost money.

56. As a result of Logan Health's conduct, Plaintiff and the Class members have suffered actual damages including from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased and imminent risk of fraud and identity theft, the lost value of their personal information, and other economic and non-economic harm.

57. Plaintiff and the Class members are therefore entitled to legal relief against Logan Health including recovery of actual damages, treble damages, injunctive relief, attorneys' fees and costs, and such further relief as the Court may deem proper.

FIFTH CAUSE OF ACTION
Unjust Enrichment

58. Plaintiff incorporate the above allegations as if fully set forth herein.

59. Plaintiff and Class Members conferred a monetary benefit on Logan Health. Specifically, they purchased services from Logan Health and in so doing provided their PII and other protected information. In exchange, Logan Health should have provided the services that were the subject of the transaction and protected Plaintiff and Class members PII with adequate data security.

60. Logan Health was aware of the benefit conferred on it by Plaintiff and Class members.

61. Logan Health's acceptance/retention of the monetary benefit it received from Plaintiff and Class members under the circumstances would render it inequitable to do so.

62. Logan Health should be compelled in equity to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received. In the alternative, Logan Health should be compelled to refund the amounts that Plaintiff and Class members overpaid for services.

SIXTH CAUSE OF ACTION
Punitive Damages

63. Plaintiff incorporate the above allegations as if fully set forth herein.

64. Logan Health's conduct in view of its previous data breach incidents constitutes "fraud" or "malice" as those terms are defined under Montana law for purposes of imposing punitive damages.

65. In addition to compensatory damages, punitive damages should be imposed in an amount sufficient to punish and deter it under Montana law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for an order:

A. certifying this case as a class action, appointing Plaintiff as Class representatives, and appointing Plaintiff's counsel to represent the Class;

B. entering judgment for Plaintiff and the Class;

C. awarding Plaintiff and Class members monetary relief including compensatory, statutory and punitive damages;

D. ordering appropriate injunctive relief;

E. awarding pre- and post-judgment interest as prescribed by law;

F. awarding reasonable attorneys' fees and costs as permitted by law;

G. granting such further and other relief as may be just and proper.

RESPECTFULLY SUBMITTED AND DATED this 9th day of March, 2022.

HEENAN & COOK

By: /s/ John Heenan

Attorneys for Plaintiff